REMARKS

Claims 15, 18, and 20 were amended. No new matter has been added.

Claims 15 to 30 are now pending. Applicants respectfully request reconsideration of the present application in view of this Amendment Response.

Applicants thank the Examiner for the comments regarding earlier conversations; and, as per a discussion with the Examiner this week, Applicants will continue the conversation regarding the present application and cited references with the Examiner in the near future.

35 U.S.C. §112, second paragraph

Claims 15, 18, and 20, were rejected under 35 U.S.C. §112, second paragraph, for indefiniteness. Claims 15, 18, and 20, have been amended above to clarify the relationship between the encryptor and crypto-module, as well as access to the Vernam key. No new matter has been added. Applicants respectfully submit that claims 15, 18, and 20, are now in proper form, and withdrawal of the rejection under 35 U.S.C. §112, second paragraph, is respectfully requested.

35 U.S.C. §103

Claims 15 to 30 were rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Patent No. 5,805,204 to Thompson ("Thompson reference") in view of U.S. Patent No. 6,285,991 to Powar ("Powar reference").

Applicants respectfully submit that amended claims 15 to 30 are allowable over the cited Thompson and Powar references.

As discussed previously, the Thompson reference is believed to refer to an interactive video guide in which object code is transmitted to set-top decoder units located in customers' homes. The Thompson reference appears to indicate that to send encrypted data, a random number is first generated by a program within the headend computer; and an appropriate imbedded key (the chosen key for the time period) is selected and loaded into the system specific algorithm. Apparently, the random number is encrypted using the DES algorithm which has been initialized and loaded with the appropriate key, producing a result which is the current system seed key. The seed key is then loaded into the system specific algorithm through which the actual transmitted data is passed. The initial random number is transmitted in clear text along with the encrypted data. When the data is received by a subscriber unit, a period identifier may be used to identify which of the keys previously and securely imbedded into the smart card will be used for the decryption process. This key must be the same one used at the headend computer for the same time period.

The Powar reference refers to an interactive electronic account statement delivery system for using over the Internet, in which the certification authority grants digital certificates to the certificated banks, which in turn grant digital certificates to billers and customers. The digital certificates form the basis for encryption and authentication of network communications, using public and private keys. The reference refers to the certificates as being stored as digital data on storage media of a customer's or biller's computer system, or contained in integrated circuit or chip cards physically issued to billers and customers.

In contrast, claim 18, for example, is directed to an encryption system, including a secret key having a defined key length; a variable parameter having a length which is a function of the defined key length; a symmetrical cipher; a Vernam key having a length that is equal to a length of a message to be protected; *the Vernam key being generated from the symmetrical cipher encryption of the secret key and the variable parameter, … the secure channel being secured by encrypting the secret key and the variable parameter with an asymmetrical cipher, the secure channel being separate from the message-transmission path; and a crypto-module including a storage space and one of the symmetrical cipher and the asymmetrical cipher, wherein the crypto-module is separate from the encryptor, the storage space is used to store the Vernam key,* and any Vernam cipher operations are performed in the encryptor, wherein the secret key and the variable parameter are communicated over at least one of the message-transmission path and the secure channel and, subsequently, used in regenerating the Vernam key, the regenerated Vernam key decrypting the message.

None of the references, alone or in combination, appear to teach or describe such a system in which a secret key and a variable parameter are devised in the manner described, e.g., as in claims 15, 18, and 20, and then transmitted via a secure channel separate from a message-transmission path. Further, none, alone or in combination, appear to teach or describe a system and method which can use the same Vernam cipher, but still have a robust system in that the Vernam key is used and then discarded after use. Further, none, alone or in combination, appear to regenerate a Vernam key from an encrypted transmitted secret key and variable parameter. Further, none, alone or in combination, appear to teach or describe using a separate storage space to store a plurality of generated Vernam keys to be used with the Vernam cipher, the use of stored information being useful in reducing the transmission time and needed resources of an encrypted message. The Thompson reference's use of an "algorithm" is not believed descriptive enough in this instance to appreciate and describe the use of a Vernam key. The Powar reference's use of a simple asymmetrical system is not analogous to the present invention in that the present invention as claimed and described herein.

Accordingly, Applicants respectfully submit that the Thompson and Powar references in combination or alone do not teach or describe all of the features of claim 18. Allowance of claim 18 is respectfully requested.

Claims 15 and 20 and dependent claims 16, 17, 19, and 21 to 30, recite features analogous to or include those of claim 18, and should be allowable for essentially the same reasons as claim 18. Accordingly, Applicants respectfully request the withdrawal of the rejection of claims 15 to 30 under 35 U.S.C. § 103(a).

CONCLUSION

For at least the foregoing reasons, Applicants respectfully submit that any outstanding rejections of claims 15 to 30 under 35 U.S.C. §§ 103(a), 112 have been overcome, and that all pending claims 15 to 30 are in condition for allowance.

It is therefore respectfully requested that the rejections be reconsidered and withdrawn, and that the present application issue as early as possible.

Respectfully submitted,

Dated: September 28, 2011

By: /Linda Lecomte/
Linda Lecomte (Reg. No. 47,084)

CUSTOMER NO. 26646

KENYON & KENYON LLP
One Broadway
New York, New York 10004
(212) 425-7200